<u>WHAT IS CLAIMED IS:</u>

1.   A method comprising:

    fabricating a first plurality of FPGA integrated circuits with a first secret key embedded by way of a first mask set; and

    fabricating a second plurality of FPGA integrated circuits with a second secret key embedded by way of a second mask set.

2.   The method of claim 1 wherein a first secure bitstream will configure properly user-configurable logic of the first plurality of FPGA integrated circuits, but not the second plurality of FPGA integrated circuits.

3.   The method of claim 1 further comprising:

    loading an unencrypted bitstream into one of the first plurality of FPGA integrated circuits to generate a secure bitstream using the first secret key.

4.   The method of claim 1 wherein the first plurality of FPGA integrated circuits with the first secret key are assigned to a first geographic area and the second plurality of FPGA integrated circuits with the second secret key are assigned to a second geographic area.

5.   The method of claim 1 wherein the first plurality of FPGA integrated circuits with the first secret key are fabricated in a first time period and the second plurality of FPGA integrated circuits with the second secret key are fabricated in a second time period, different from the first time period.

6.   The method of claim 1 wherein only one mask differs between the first and second mask sets.

7.   The method of claim 1 wherein the first plurality of FPGA integrated circuits with the first secret key are assigned exclusively to a first customer.

8.   The method of claim 5 wherein the first time period is about the same duration as the second time period.

9.   The method of claim 5 wherein the first time period is a different duration from the second time period.

29

1   10.   The method of claim 6 wherein the one mask is a contact mask.

1   11.   The method of claim 1 wherein there are random differences
2 between artwork of the first and second plurality of FPGA integrated circuits in addition
3 to the different embedded secret keys.

1   12.   The method of claim 1 wherein the first and second secret keys are
2 presented on wires of respective plurality of FPGA integrated circuits for only a limited
3 duration.

1   13.   The method of claim 1 wherein the first secret key is embedded by
2 setting an initial state of a selection of memory cells in a device configuration memory of
3 the FPGA integrated circuit.

1   14.   The method of claim 1 wherein the first secret key is embedded by
2 changes to a relatively large block of logic in the first plurality of FPGA integrated
3 circuits and its value extracted using a CRC algorithm.

1   15.   The method of claim 13 further comprising:
2   extracting the first secret key by using a CRC algorithm to compute a
3 checksum of the initial state of the device configuration memory.

1   16.   The method of claim 1 further comprising:
2   loading an unencrypted bitstream into one of the first plurality of FPGA
3 integrated circuits to generate a secure bitstream based on the first secret key and an on-
4 chip generated random number.

1   17.   The method of claim 1 further comprising:
2   loading an unencrypted bitstream into one of the first plurality of FPGA
3 integrated circuits to generate a secure bitstream based on the first secret key and an on-
4 chip generated random number, wherein the secure bitstream includes a message
5 authentication code.

1   18.   A method comprising:
2   embedding a first secret key within the artwork of an FPGA integrated
3 circuit;

4   storing a user-defined second secret key within an encrypted FPGA

5 bitstream stored in an external nonvolatile memory accessible by the FPGA;

6   decrypting the user-defined second secret key using the first secret key;

7 and

8   setting up a secure network link between the FPGA and a server using the

9 user-defined second secret key.

1   19.   The method of claim 18 further comprising:

2   downloading an FPGA bitstream using the secure network link;

3   encrypting the downloaded FPGA bitstream using the first secret key; and

4   storing the encrypted downloaded bitstream in the external memory.

1   20.   The method of claim 18 wherein the secure network link is created

2 using a standard internet security protocol.

1   21.   The method of claim 18 further comprising:

2   configuring the FPGA using the encrypted downloaded bitstream stored in

3 the external memory.

1   22.   A method comprising:

2   storing a first secret key on an FPGA chip;

3   causing the FPGA to calculate a message authentication code (MAC)

4 corresponding to a user design; and

5   storing the message authentication code with bitstream information in a

6 nonvolatile memory.

1   23.   The method of claim 22 further comprising:

2   storing copyright messages with the bitstream information;

3   detecting unauthorized alterations to the bitstream using the message

4 authentication code; and

5   preventing bitstreams which have been altered from being used to

6 configure an FPGA.

1   24.   The method of claim 22 further comprising:

2   recording the message authentication code along with corresponding

3 identification information for a product containing the FPGA; and

31

4   examining the message authentication code stored in the nonvolatile

5   memory of a product containing a pirated FPGA design, which will enable determining

6   the identity of the customer to whom the pirated FPGA was originally supplied using a

7   record of MACs and corresponding product identification.